In the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (canceled).

2. (currently amended) The method of claim 31 [[1]], including ~~distributing symmetric encryption keys for use in a plurality of communication sessions using respective pluralities of exchanges, and~~ using said associated session key in response to another request to initiate a communication session from a third station received by the first station ~~for first exchanges in the respective pluralities of exchanges for initiating communication sessions in the plurality of communication sessions initiated with the first station,~~ during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

3. (previously presented) The method of claim 2, including associating a unique set of intermediate data keys with each session key.

4. (currently amended) The method of claim 31 [[1]], including:

providing a buffer at the first station;

storing the ~~an ephemeral~~ set of ephemeral session keys in the buffer; and ~~for respective session key lifetimes;~~

~~associating respective session key initiation intervals with said session keys stored in said buffer;~~

~~using session keys from the set of session keys from said buffer as session keys in response to requests received by said first station during said respective, associated session key initiation intervals;~~

removing session keys from said buffer upon expiry of [[the]] respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals.

5. (canceled).

6. (currently amended) The method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges ~~for the plurality of exchanges used to distribute the symmetric encryption key for use in a communication session can be completed~~ in expected circumstances.

7. (currently amended) The method of claim 4, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges ~~for the plurality of exchanges used to distribute the symmetric encryption key for use in a communication session can be completed~~ in expected circumstances, where M is less than or equal to 10.

8. (canceled).

9. (currently amended) The apparatus of claim [[8]] 34, including logic to ~~distribute symmetric encryption keys for use in a plurality of communication sessions using respective pluralities of exchanges, and to~~ use said associated session key in response to another request to initiate a communication session from a third station received by the first station ~~for first exchanges in the respective pluralities of exchanges for distributing the symmetric encryption keys in the plurality of communication sessions initiated with the first station,~~ during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

10. (previously presented) The apparatus of claim 9, including logic to associate a unique set of intermediate data keys with each session key.

11. (currently amended) The apparatus of claim [[8]] 34, including

a buffer at the first station;

logic to store the ~~an ephemeral~~ set of ephemeral session keys in the buffer ~~for respective session key lifetimes, to associate respective session key initiation intervals with particular~~

~~session keys in said set of session keys stored in said buffer, to use session keys from said buffer as session keys in response to requests received by said first station during said respective session key initiation intervals,~~ and to remove session keys in said set of ephemeral session keys from said buffer after expiry of the respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals.

12. (canceled).

13. (currently amended) The apparatus of claim 11, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges ~~for the plurality of exchanges used to distribute the secret encryption key for use in a communication session can be completed~~ in expected circumstances~~, and including logic to remove said session keys in said set of session keys from said buffer after expiry of the session key lifetimes~~.

14. (currently amended) The apparatus of claim 11, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges ~~for the plurality of exchanges used to distribute the secret encryption key for use in a communication session can be completed~~ in expected circumstances~~, and including logic to remove said session keys in said set of session keys from said buffer after expiry of the session key lifetimes~~.

15. (canceled).

16. (currently amended) The article of claim [[15]] 37, wherein the instructions include logic to ~~distribute secret encryption keys for use in a plurality of communication sessions using respective pluralities of exchanges, and to~~ use said associated session key in response to another request to initiate a communication session from a third station received by the first station ~~for first exchanges in the respective pluralities of exchanges for assigning secret encryption keys in the plurality of communication sessions initiated with the first station,~~ during said particular

session key initiation interval, and using other session keys from the set of ephemeral session keys after expiry of said particular session key initiation interval.

17. (previously presented) The article of claim 16, wherein the instructions include logic to associate a unique set of ephemeral intermediate data keys with each session key.

18. (currently amended) The article of claim [[15]] 37, wherein

the first station includes a buffer; and

the instructions include logic to store [[a]] the set of ephemeral session keys in the buffer ~~for respective session key lifetimes, to associate respective session key initiation intervals with particular session keys in said set of session keys stored in said buffer, to use session keys from said buffer as session keys in response to requests received by said first station during said respective session key initiation intervals,~~ and to remove session keys in said set of ephemeral session keys from said buffer after expiry of the respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals.

19. (canceled).

20. (currently amended) The article of claim 18, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges ~~for the plurality of exchanges used to distribute the secret encryption key for use in a communication session can be completed~~ in expected circumstances~~, and the instructions include logic to remove said session keys in said set of session keys from said buffer after expiry of the session key lifetimes~~.

21. (currently amended) The article of claim 18, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges ~~for the plurality of exchanges used to distribute the secret encryption key for use in a communication session can be completed~~ in expected circumstances~~, and the instructions include logic to remove said session keys in said set of session keys from said buffer after expiry of the session key lifetimes~~.

22-30. (canceled).

31. (new) A method for mutual authentication in communications between first and second stations, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and if mutual authentication is verified at the first station, then sending a message indicating successful authentication.

32. (new) The method of claim 31, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

33. (new) The method of claim 31, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication ~~in~~ communications between the first and second stations in the communication session.

34.(new) A data processing apparatus, comprising:

a processor associated with a first station, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;

logic to provide for mutual authentication in communications between the first station and a second station, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), ~~and~~ decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and

if mutual authentication is verified at the first station, then sending a message indicating successful authentication.

35. (new) The apparatus of claim 34, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

36. (new) The apparatus of claim 34, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session.

37. (new) An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;

logic to provide for mutual authentication in communications between the first station and a second station, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals;

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval;

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n), calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and if mutual authentication is verified at the first station, then sending a message indicating successful authentication.

38. (new) The apparatus of claim 37, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i).

39. (new) The apparatus of claim 37, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session.

///